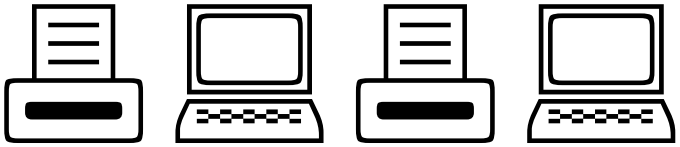

HIPAA

A GUIDE TO PRIVACY READINESS, v3

The MARYLAND HEALTH CARE COMMISSION

Rex W. Cowdry, M.D.
Executive Director

Revised October 2009

Commissioners

Marilyn Moon, Ph.D., Chair
Vice President and Director, Health Program
American Institutes for Research

Garret A. Falcone, Vice Chair
Executive Director
Charlestown Retirement Community

Reverend Robert L. Conway
Retired Principal and Teacher
Calvert County Public School System

John E. Fleig, Jr.
Director
United Healthcare

Tekedra McGee Jefferson, Esquire
Assistant General Counsel
AOL LLC

Kenny W. Kan
Senior Vice President/Chief Actuary
CareFirst BlueCross BlueShield

Sharon Krumm, R.N., Ph.D.
dministrator & Director of Nursing
The Sidney Kimmel Cancer Center
Johns Hopkins Hospital

Robert Lyles, Jr., M.D.
Medical Director
LifeStream Health Center

Barbara Gill McLean, M.A.
Retired, Senior Policy Fellow
University of Maryland School of Medicine

Roscoe M. Moore, Jr., D.V.M., Ph.D., D.Sc.
Retired, U.S. Department of Health
and Human Services

Kurt B. Olsen, Esquire
Klafter and Olsen LLP

Sylvia Ontaneda-Bernales, Esquire
Ober, Kaler, Grimes, & Shriver

Darren W. Petty
President
Maryland State United Auto Workers
General Motors/United Auto Workers

Nevins W. Todd, Jr., M.D.
Cardiothoracic and General Surgery
Peninsula Regional Medical Center

Randall P. Worthington
President/Owner
York Insurance Services, Inc.

HOW TO USE PRIVACY GUIDE

This guide is the effort of the Maryland Health Care Commission to assist the health care industry in meeting privacy requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Users are encouraged to implement privacy standards in a manner reasonable and consistent to their organizational size and structure. The Maryland Health Care Commission would like to acknowledge the EDI/HIPAA Workgroup, representing payer, provider, and clearinghouse organizations and individuals throughout the State of Maryland in the development of *"A Guide to Privacy Readiness, v3."*

Format

Section IV. Assessment Guide and Work Plan

Table Layout

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA Readiness	INDUSTRY DEVELOPED STRATEGY To Assist Practitioners & Facilities
Description of standard Citation Category of standard=SEE BELOW 1-Operational 2-Consumer Control 3-Administration	Quoted regulatory language User question to assess readiness ► Extra clarification of regulatory language	Checklist for user question ☐ ☐ **YES NO**	Suggestions for implementation **Sample Policy & Procedure**

1. **Operational standards** define use and disclosure of medical information (pages 1-7).
2. **Consumer Control standards** outline an individual's privacy rights in the use and disclosure of their medical information (pages 7-11).
3. **Administration standards** define the requirements for documentation, staff training, and administering complaints (pages 11-20).

Self Assessment: Rank your readiness to comply with privacy regulations on page 33.

I. INTRODUCTION

Background

On August 21, 1996, President Bill Clinton signed into law the Health Insurance Portability and Accountability Act of 1996. One part of this law, Administrative Simplification, is intended to standardize electronic health care transactions, protect the privacy of patient identifiable information, and ensure the security of electronic information. HIPAA also covers the confidentiality of a person's identifiable health information via electronic media. The privacy rule encompasses medical records and other individually identifiable health information held or disclosed by health plans, health care clearinghouses, and health care providers, in any form, whether communicated electronically, on paper, or orally. The final privacy regulations took effect on April 14, 2003.

HIPAA Privacy Regulations Overview

The HIPAA Privacy Regulations provide patients with significant rights to better understand and control how their health information is used and disclosed. Summarized below are the leading standards provided by the final rule.

- Providers are required to provide patients with a clearly written explanation of how their medical information will be used, kept, and disclosed.
- In the absence of a signed consent, providers must make a "good faith effort" to obtain written acknowledgement of receipt of the provider's Notice of Privacy Practices that describes their use of PHI.
- Disclosure of patient information must be limited to the minimum necessary to comply with the request.
- Patients have the right to complain to a health care provider or to the Secretary of Health and Human Services within 180 days of the known violation.
- Under ordinary circumstances, patients must be able to access, duplicate, and request an amendment to their medical records. Other than for treatment, payment, and health care operations, providers must make a history of disclosures available upon patient request only if an authorization has not been signed.
- Authorizations are requested for non-routine disclosures of patient information with exceptions only for treatment, payment, and health care operations.
- Policies and procedures must include a process for disclosing protected health information that include steps to assure that business associates maintain the privacy of protected health information.
- Providers must establish written policies and procedures documenting compliance with the privacy standards.
- A Privacy Official must be designated with the responsibility of ensuring that employees receive sufficient awareness training and instruction on the new privacy protection procedures.
- Health care providers must provide a means for patients to inquire or make complaints to the practice regarding the privacy of their medical records.
- Criminal penalties for PHI privacy violations range from $50,000 and one year in prison to $250,000 and up to 10 years in prison, depending upon the severity of the disclosure.

Application

The Maryland Health Care Commission's, "A Guide to Privacy Readiness, v3" is intended to assist most practitioners and small facilities in their privacy assessment. The third edition of "A Guide to Privacy Readiness, v3" contains significant changes to Section V, ARRA Addendum to HIPAA Privacy Guide, which includes the changes originating from the passage of the Federal *American Recovery and Reinvestment Act of 2009* (ARRA), which was signed into law by President Barack Obama on February 17, 2009. The bill addresses areas such as the reporting of a breach of security or privacy of unsecured PHI, the inclusion of business associate's with the reporting of breaches, and the disclosure of "minimum necessary" PHI.

II. Maryland Law on the Confidentiality of Medical Records

Did you know that Maryland has a privacy law…

- All medical records are considered protected information. This includes both electronic and paper records and also oral communications.
- Patient rights over their medical information include patient-provider medical records confidentiality, permitting patient access to their medical files, and allowing patients to add or alter their medical records according to those procedures established by the provider.
- Health care providers may only disclose medical records upon receipt of patient notification. Health care providers are prohibited from disclosing any patient identifiable information to a person for educational or research purposes, evaluation and management, or accreditation of a facility unless an acknowledgement not to redisclose is received.
- Any health care provider or other person(s) who knowingly and willfully violate the provisions of Maryland's Medical Records Law are guilty of a misdemeanor. If convicted, the violator is subject to a fine not exceeding $1,000 for the first offense and $5,000 for each subsequent conviction.
- Copies of medical records are permitted upon patient request.
- A health care provider may disclose medical records about a patient without authorization when seeking payment for health care services, in emergency situations, to the provider's legal counsel, coordinating benefit payments, or to a unit of state or local government for purposes of investigation. Health care providers must disclose medical records in situations pertaining to criminal investigation, or to an appropriate organ, tissue, or eye recovery agency.
- A facility director may confirm or deny the presence of an individual to a parent, guardian, next of kin, or any individual who has significant interest in the individual's status. State or local government agencies may report the status of an individual in cases of missing persons where a report has been filed.
- Information may be released without consent in circumstances of investigations or treatment in cases of suspected abuse or neglect of a child or adult and also in the licensure/certification or discipline of a health professional.
- Personal notes for mental health therapy that are kept separate from the medical record are not considered part of the medical record. Mental health information subject to disclosure includes information concerning diagnosis, treatment plans, symptoms, prognosis, or progress updates.
- A health care provider or any other person who knowingly and willfully requests or obtains a medical record under false pretenses or through deception, or knowingly and willfully discloses a medical record is subject to a fine not exceeding $50,000 or imprisonment for not more than one year or both. If the offense is committed under false pretenses, a fine not exceeding $100,000 or imprisonment for five years or both may apply. If the offense is committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious intent, penalties include up to a $250,000 fine or imprisonment for not more than 10 years or both.

III. Glossary of HIPAA Terms

Term	Description
Authorization	A document signed by the patient authorizing the release of specific protected health information (PHI). Authorizations must outline what information is being disclosed, the recipient of the information, expiration date, a statement of the individual's right to revoke, a statement describing potential re-disclosure of the information, and dated signature of individual or guardian. If signed by guardian, the authorization must describe the relationship. An authorization would be necessary for pre-employment physicals, research, and psychotherapy notes.
Business Associate	A person or entity using protected health information (PHI) to perform a function or activity on behalf of a provider/facility, health plan or clearinghouse but who is not part of the aforementioned workforce. Examples of services performed by business associates are billing, practice management, and utilization review.
Consent	Eliminated in final modifications to HIPAA privacy regulations since it would have prevented care to anyone who refused to give consent for treatment, payment, and health care operations. The regulation now requires health care providers to use good faith efforts in obtaining an individual's written acknowledgment of their Notice of Privacy Practices.
Covered Entity	A facility, health plan, or health care clearinghouse that transmits medical information in electronic form. (***Referred to as health care provider in this document).***
DHHS	The Department of Health and Human Services.
Data Aggregation	A business associate's combining of protected health information (PHI) created or received in its capacity as a business associate of a provider/facility, health plan, or health care clearinghouse for the purpose of data analyses relating to the health care operations of the respective entity.
Data Content	All data elements and code sets built-in to a transaction, and not related to the format of the transaction.
Direct Treatment Relationship	An exclusive treatment association between an individual and a health care provider.
Disclosure	External release or divulgence of protected health information by a medical office to another entity.
Facility Directory	A list of inpatients admitted to a facility. Directory may include the patient's name, location, general status, and religious affiliation. For requests by patient name and where a patient has not objected to inclusion, facility can disclose the patient location and general status. Religious affiliation may only be shared with clergy.
Health Care	Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative medical care, services or supplies with respect to the physical or mental condition or functional status of an individual. Under HIPAA, health care includes the sale or dispensing of a drug, device equipment, or other item in accordance with a prescription.

Health Care Clearinghouse	A public or private entity that processes or facilitates the processing of information received from a medical office in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. Also encompasses public or private entities that may receive a standard transaction from another party and processes or facilitates the processing of that information into nonstandard format or nonstandard data content for a receiving party.	
Health Care Operations	Health care operations include the administrative activities of a medical office to the extent that the activities are related to covered functions, as well as any operations of an organized health care arrangement involving the medical office, such as: ♦ Quality assessment and improvement ♦ Evaluations of practitioner or provider performance for competence ♦ Business planning and development	♦ Underwriting, premium rating, and other activities relating to creation, renewal, or replacement of a contract of health insurance ♦ Business management and general administrative activities ♦ Compliance management of HIPAA requirements ♦ Resolution of internal grievances ♦ Sale, transfer, merger, or consolidation of all or part of a medical office
Health Care Provider	A provider or facility of medical services who furnishes, bills, or is paid for health care in the normal course of business, including institutional practitioners in home health agencies, clinics, rehabilitation & skilled nursing facilities, clinical laboratories, pharmacies, nursing homes, and suppliers of durable medical equipment.	
Health Information	Any form or medium of oral or recorded protected health information (PHI) on an individual created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse. This relates to the past, present, or future physical or mental health or condition of an individual and does include provisions for payment of services.	
Health Plan	An individual or group plan that provides, or pays the cost of medical care.	
Indirect Treatment Relationship	An association between an individual and medical office in which a health care provider delivers care based on the orders of another health care provider; or circumstances where services, products, or associated health services are provided by another medical office and then related to the practitioner directly interacting with the individual.	
Individual	A person who is the subject of protected health information.	
Individually Identifiable Health Information (IIHI)	Any subset of health information collected on an individual, including demographics or other potentially identifying matter, that is created or received from a health care provider, health plan, employer, or health care clearinghouse and relates to the past, present or future physical or mental health or condition of the individual. Also referred to as **Protected Health Information.**	

Marketing	A communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Exclusions to marketing under HIPAA include: (1) health-related products provided by the practitioner that are included in the individual's health plan benefits; (2) for the treatment of that individual; or (3) for case management/care coordination, or to recommend advantageous alternative therapies, providers, or settings of care to an individual.
Organized Health Care Arrangement	A clinically integrated care setting in which individuals receive health care from more than one practitioner. Examples of health care in which more than one practitioner participates include: HMO or group health plans, utilization reviews, quality assessment and improvement activities, and payment activities for the purpose of administering the sharing of financial risk.
Payment	Actions taken by a health plan to obtain premiums or to fulfill its responsibility for coverage or actions taken by a health care provider or health plan to obtain or provide reimbursement for health care services.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) transmitted or maintained by a medical office *excluding* education records covered under the Family Educational Right and Privacy Act. Also exempt are employment records held by a medical office in its role as employer. **(Refer to "Individually Identifiable Health Information")**
Psychotherapy Notes	Recorded notes (in any medium) of a mental health professional documenting or analyzing the contents of conversations during private, group, joint or family counseling sessions. Psychotherapy notes exclude medication, session start and stop times, modalities and frequency of treatments, results of clinical tests and summaries of diagnosis, functional status, treatment plans, symptoms, prognosis and progress.
Research	A methodical investigation, including research development, testing and evaluation, designed to develop or contribute to theory analysis.
Transaction	The transmission of information between two parties to carry out financial or administrative activities related to health care.
Treatment	Provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a medical office with a third-party; consultation between health care providers relating to a patient, or the referral of a patient from one medical office to another.
Use	The sharing, employment, application, utilization, examination or analysis of protected health information within a medical office.
Workforce	Employees, volunteers, trainees, and other persons performing work for a medical office and under direct control of the medical office whether paid or not.

IV. ASSESSMENT GUIDE AND WORK PLAN

This section incorporates DHHS amendments to HIPAA Privacy Rule released August 14, 2002.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Uses & Disclosures of Protected Health Information (PHI) §164.502(a) Operational	***Final privacy rules require health care providers to obtain a signed consent or use good faith efforts to obtain an individual's written acknowledgment of receipt of the Notice of Privacy Practices. The law encourages the development of a comprehensive document outlining the use of PHI for treatment, payment, and health care operations layered with a summarized version for acknowledgement purposes. The good faith effort must be made at the time of the first delivery of the Notice of Privacy Practices and acknowledgement or efforts to obtain it must be documented.*** **? Have you established a comprehensive Notice of Privacy Practices ?** Clarification: In place of consent (to be used discretionally), health care providers are asked to establish a detailed Notice of Privacy Practices explaining how PHI is handled for treatment, payment, and health care operations. In addition, when treating a mutual patient, providers are permitted to exchange information in order to obtain payment, or for operational purposes such as quality assurance. Authorizations remain a requirement for use or disclosure of PHI for other than treatment, payment, or health care operations.	☐ **Yes**	☐ **No**	♦ Prepare a detailed Notice of Privacy Practices document specifically outlining the intended use of PHI for treatment, payment, and health care operations. ♦ Develop an acknowledgment document that briefly explains the Notice of Privacy Practices, and request a signed notice of information from the individual. ♦ Document instances where the patient or personal representative declined signing the acknowledgement. **Sample Policy & Procedure** Refer patients to the **Notice of Privacy Practices** for specific information regarding handling of **PHI** and ask the patient to acknowledge receipt of the information in writing.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Uses & Disclosures for which an authorization is required §164.508 Operational	***Core Elements of an authorization are: A specific description of the information to be disclosed, the name or other specific identification of the person(s) making the request, expiration date, a statement of the individual's right to revoke, statement that information used or disclosed may be subject to re-disclosure, signature and date. Authorizations signed by a representative must include a description of the authority.*** **? Does your *authorization document contain the required detail for specific disclosures of PHI ?*** Clarification: Individuals must authorize the use or disclosure of particular PHI, such as that released for pre-employment physicals, research involving treatment, and psychotherapy notes. One form can be used for uses or disclosures requested by the individual and also for uses and disclosures requested by or from the health care provider, including that for clinical research. All required elements must be included for an authorization to be valid.	☐ **Yes**	☐ **No**	♦ Develop an authorization form that outlines all requirements for the release of PHI and specifies the information to be used or disclosed so there is no doubt by the individual or your office staff as to what is being released. ♦ Develop separate policies and procedures for obtaining authorization for the use and disclosure of psychotherapy notes. **Sample Policy & Procedure** An authorization form is required for the release of **PHI** for pre-employment physicals, research involving treatment, and psychotherapy notes. An authorization must specify the information being used or disclosed, the recipient of the information, expiration date, a statement of the patient's right to revoke, and dated signature.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Minimum Necessary §164.502(b) §164.514(d) Operational	***A health care provider must limit use and disclosure of PHI to the minimum necessary to carry out the intended purpose of the request.*** **? Are you and/or your staff aware of what is considered "minimum necessary" for the various disclosures of PHI ?** Clarification: Minimum necessary means using professional judgment to make a discerning effort to restrict information to the amount necessary to accomplish the intended use or disclosure. Minimum necessary does not apply to health care providers providing treatment to a mutual patient.	☐ **Yes**	☐ **No**	♦ Update policies on the disclosure of PHI and instruct workforce members to restrict the release of PHI to only documents related to a specific request, i.e. claims payment. ♦ Use actual examples to simulate what is appropriate to release under the "minimum necessary" requirements. **Sample Policy & Procedure** Restrict the use or disclosure of **PHI** to the minimum necessary to accomplish the purpose specified in the authorization.
Disclosures to Business Associates §164.502(e) Operational	***Disclosures of PHI may be made to business associates where a Business Associate Contract is in place.*** **? Can you identify situations where a Business Associate Contract would be necessary ?** Clarification: Business Associate Contracts are applicable in situations where a health care provider employs an outside person or entity to perform functions where they are not providing medical care and there is indirect access to PHI. This type of agreement is not necessary between health care providers providing treatment to a mutual patient or between a medical office and payer for payment purposes.	☐ **Yes**	☐ **No**	♦ Modify or add language to existing trading partner agreements incorporating privacy standard requirements for the use or disclosure of PHI. ♦ Implement Business Associate Contracts with all outside entities performing services for your office. **Sample Policy & Procedure** Organization(s) not directly involved with patient care but have access to **PHI** must sign a **Business Associate Contract** upon initial contracting or at contract renewal. Examples: Building maintenance and janitorial services, medical transcribers.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object §164.510 Operational	***Health care providers may disclose PHI without an individual's authorization when used for facility directories released to clergy and other visitors, or to update family members and others involved in the individual's care.*** **? Does your Notice of Privacy Practices clearly describe the limited situations where PHI can be freely used or disclosed ?** Clarification: Individuals must be provided the opportunity to prohibit or restrict certain disclosures of PHI. State law precludes HIPAA requirements for disclosures where parent/guardian authorization is required.	☐ **Yes**	☐ **No**	♦ Use the ***Notice of Privacy Practices*** document to describe situations where PHI can be used or disclosed without patient authorization and provide the option for individuals to object. **Sample Policy & Procedure** Practitioners can use common practice rules to make decisions to release **PHI** to parents or guardians of minors in instances where state law is silent.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Uses and Disclosures for which consent, an authorization, or opportunity to agree or object is not required §164.512(a) – (l) Operational	***A health care provider may use or disclose protected health information without an individual's written authorization in the following circumstances:*** ***(a) Uses and disclosures required by law*** ***(b) Uses and disclosures for public health activities*** ***(c) Disclosures about victims of abuse, neglect or domestic violence*** ***(d) Uses and disclosures for health oversight activities*** ***(e) Disclosures for judicial and administrative proceedings*** ***(f) Disclosures for law enforcement purposes*** ***(g) Uses and disclosures about decedents*** ***(h) Uses and disclosures for cadaver organ, eye or tissue donation purposes*** ***(i) Uses and disclosures for research purposes*** ***(j) Uses and disclosures to avert a serious threat to health or safety*** ***(k) Uses and disclosures for specialized government functions*** ***(l) Disclosures for workers' compensation*** **?** ***Are you and/or your workforce familiar with the special circumstances that would allow the disclosure of PHI without authorization ?*** Clarification: The regulations are designed to reflect the importance of safeguarding individuals' confidentiality while enabling important activities that require protected health information to proceed, such as public health oversight.	☐ **Yes**	☐ **No**	♦ Prepare guidelines that outline the HIPAA standards for allowing the use and disclosure of PHI without authorization. ♦ Convey this information to individuals in the ***Notice of Privacy Practices***. **Sample Policy & Procedure** Non-routine requests for **PHI** must be approved by the practice administrator.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
De-identification of PHI §164.514(a) Operational	***Individual health information loses its HIPAA protections and may be used or disclosed freely if it cannot be used to identify an individual.*** **? Are you aware of the 19 elements that de-identify PHI data and frees it for disclosure ?** <u>Clarification:</u> Health care providers are permitted to use PHI once it has been stripped of all elements that could potentially identify the individual who is the subject of the protected information. The 19 identifiers are: 1. Name 2. All address information 3. E-mail addresses 4. Dates (except year) 5. Social Security Number 6. Medical record numbers 7. Health plan beneficiary numbers 8. Account numbers 9. Certificate numbers 10. License numbers 11. Vehicle identifiers 12. Facial photographs 13. Telephone numbers 14. Device identifiers 15. URLs 16. IP addresses 17. Biometric identifiers 18. The geographic unit formed by combining all zip codes with the same three initial digits containing more than 20,000 people and the initial three digits of all geographic units with fewer than 20,000 people is changed to 000. 19. Any other unique identifying number, characteristic, or code and the health care provider does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.	☐ **Yes**	☐ **No**	♦ Implement a release of information policy that requires preauthorization by your practice administrator. ♦ Use the 19 elements to create a checklist when preparing de-identifiable data files. **<u>Sample Policy & Procedure</u>** **PHI** is routinely used for treatment, payment, and health operations. All other requests for **PHI** are to be reviewed by the practice administrator who is responsible for taking the appropriate steps to de-identify **PHI**.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Uses and Disclosures of PHI for Marketing §164.508(a)(3) Operational	***Health care providers must obtain authorization prior to any communications which constitute marketing or targeted fund raising activities.*** **? Have you identified products and services offered by you that represent marketing ?** Clarification: Health care providers are required to obtain an individual's specific authorization prior to sending marketing materials. Communications made to an individual for case management or care coordination, communications to describe a health-related product or service, and/or communications made to an individual for treatment purposes are excluded from the marketing definition.	☐ **Yes**	☐ **No**	♦ Include your marketing and fund raising policy in the ***Notice of Privacy Practices***. Identify marketing practices allowed without patient authorization, such as face-to-face encounters and examples of products with nominal value. ♦ Present your office policy in supporting promotional events or items in the ***Notice of Privacy Practices***. ♦ Prepare an authorization form that specifically requests an individual's preference concerning marketing. ♦ Obtain an individual's authorization before releasing PHI to business associates for marketing purposes. ♦ Obtain an individual's authorization before using PHI to perform targeted fund raising activities. **Sample Policy & Procedure** Obtain marketing preference in a signed authorization from individuals at the time of registration.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Notice of Privacy Practices for PHI §164.520 Operational	***Health care providers must provide individuals with Notice of Privacy Practices and a good faith effort to obtain written acknowledgment of receipt. Notice of Privacy Practices acknowledgement required with or without the optional consent.*** **? Have you established a Notice of Privacy Practices document and a process for assuring that this information reaches every individual seen in your office ?** Clarification: Health care providers are required to develop a written notice of information practices that details the types of uses and disclosures that will be made with PHI. The notice should inform individuals what is done with their PHI and their rights under HIPAA law with respect to that information. The Notice of Privacy Practices should be given to individuals at registration. Health care providers that are part of organized health care arrangements may use a joint notice. Health care providers must archive copies of the notices for six years.	☐ **Yes**	☐ **No**	♦ Develop a policy manual to specifically define all the elements referred to in the ***Notice of Privacy Practices***. ♦ Prepare an abbreviated copy of the full ***Notice of Privacy Practices*** and request a signed acknowledgment. The full notice must follow. ♦ If customer services or benefits are advertised electronically, prominently post the ***Notice of Privacy Practices*** on web site. **Sample Policy & Procedure** Offer the **Notice of Privacy Practices** during registration and request a signed receipt.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Rights to Request Privacy Protection for PHI §164.522(a) Consumer Control	***A health care provider must accommodate PHI requests by individuals who wish restrictions on (1) use and disclosure for treatment, payment, and health care operations (2) disclosures permitted for involvement in the individual's care and notification purposes.*** **? Do you fully understand your rights and those of patients who may request restrictions on the use and disclosure of their PHI ?** Clarification: Requested restrictions by an individual must be retained for six years. A health care provider is not required to agree to an individual's restrictions but if they do, the health care provider must abide except in emergency situations. Health care providers may terminate a restriction agreement upon notifying the individual of if the individual consents to or requests termination.	☐ **Yes**	☐ **No**	♦ Carefully review use and disclosure practices with individuals as part of the initial visit. ♦ Clearly indicate in the ***Notice of Privacy Practices*** an individual's right to request restrictions on the use and disclosure of their PHI, and that the health care provider is not required to agree with the requested restrictions. **Sample Policy & Procedure** Provide the **Notice of Privacy Practices** to accommodate specific patient wishes to place limitations on the use of their **PHI**.
Confidential Communications Requirements §164.522(b) Consumer Control	***A health care provider must provide individuals the opportunity to receive PHI communications by alternative means or at alternative locations and oblige all reasonable requests.*** **? Can you accommodate individuals requesting to receive PHI communications by alternative means ?** Clarification: This standard offers alternatives to individuals who wish to receive communications of PHI by alternative means or at an alternative address.	☐ **Yes**	☐ **No**	♦ Verify contact and address information as part of scheduling office visits to assure current patient information. ♦ Provide an option on the registration form to accommodate an individual's request for discretion when being contacted. **Sample Policy & Procedure** Provide a statement in the **Notice of Privacy Practices** that patients will be contacted one business day prior to a scheduled appointment using their home telephone.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Access of Individuals to PHI §164.524 Consumer Control	***Individuals are entitled to inspect and copy PHI, in whole or in part, for as long as the health care provider maintains the information.*** **? Are your medical files managed in a way that allows for patient inspection and/or release of PHI ?** Clarification: Health care providers must establish policies and procedures to ensure that individuals understand and can be involved in the handling of their PHI. Circumstances where individuals do not have the right to access PHI include: (1) psychotherapy notes; (2) information pertaining to criminal, civil, or administrative actions; (3) PHI lawfully prohibited from release because it is subject to or exempted from Clinical Laboratory Improvements Amendments (CLIA); (4) information created by someone other than the provider or given to the provider under a promise not to release. A health care provider must act on requests for onsite information within 30 days of receipt, and 60 days otherwise. Under certain conditions, health care providers may apply a self-imposed 30-day extension. An individual's request for PHI can be denied for extreme reasons, such as information that may endanger life or well-being. Denied requests are subject to the individual's review and health care providers are required to arrange an unbiased opinion by another health professional. This opinion must be administered timely with written notice and outcome furnished to the individual. Upon prior approval from the individual, fees may be applied to the cost of copying, mailing, and summary preparation. A health care provider must retain detailed documentation of the review in an accessible format for six years.	☐ **Yes**	☐ **No**	♦ Notify individuals in the ***Notice of Privacy Practices*** of their right to access their PHI for the previous six years. ♦ Establish protocol to document individual requests for accessing PHI including incurred costs. **Sample Policy & Procedure** Dedicate a section of your **Notice of Privacy Practices** to inform individuals of their right to access PHI and the administrative fees incurred.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Amending PHI §164.526 Consumer Control	***Individuals have the right to request amendments to PHI in a designated record set for as long as the health care provider maintains the information.*** **? Are you aware of your obligations and rights should an individual request amendments to their medical record ?** Clarification: Health care providers must establish policies and procedures to ensure that individuals understand and can be involved in amending their PHI. Circumstances where individuals do not have amendment rights include (1) information not created by the health care provider (unless individual claims the originator of the PHI is no longer available to amend); (2) the PHI is not part of the designated record set; (3) the PHI was unavailable for inspection; (4) the PHI is accurate and complete. A health care provider may require an individual to make the request in writing and provide a reason. Requests for information must be responded to within 60 days of receipt, and under certain conditions, a self-imposed 30-day extension may be applied. If granted, a health care provider must properly notify the individual and, to the extent possible, all relevant persons, including business associates. For denied requests for amendment, the health care provider must provide the individual with timely written notice explaining the reason for denial and the individual's right to rebuttal. Likewise, a health care provider can file a rebuttal provided the individual is notified. Amendment documentation is subject to a 6-year retention timeframe.	☐ **Yes**	☐ **No**	♦ Notify individuals in the ***Notice of Privacy Practices*** of their right to request amendments to PHI and review the process for making such a request. ♦ Establish protocol to document and retain an individual's request to amend PHI. **Sample Policy & Procedure** Individuals should be informed that requests to amend **PHI** must be made in writing and a written response should be received from the doctor's office within 60 days.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Accounting of Disclosures of PHI §164.528 Consumer Control	***Individuals can request an account of PHI disclosures made by a health care provider in the six years prior to the request. This does NOT include disclosures: (1) for treatment, payment, and health care operations (2) to the individual (3) pursuant to an authorization (4) for the facility's directory or to persons involved in the individual's care (5) for national security or intelligence purposes (6) to correctional institutions or law enforcement officials (7) as part of a limited data set, and (8) information accrued prior to the HIPAA compliance date.*** **? Do you document individual PHI disclosures as outlined above ?** Clarification: Health care providers must act on an individual's request for a listing of PHI uses and disclosures within 60 days, with possible 30-day extensions as described for accessing PHI. The health care provider must provide individuals with the first account at no charge. For subsequent requests, within a 12-month period, the health care provider may charge a reasonable, cost-based fee.	☐ **Yes**	☐ **No**	♦ Detail PHI disclosures in individual medical records and include date and to whom disclosure was made. ♦ Use the ***Notice of Privacy Practices*** to inform individuals of their right to access a disclosure log of their PHI. **Sample Policy & Procedure** Individuals must make a written request to receive a history of **PHI** disclosures. The doctor's office must provide monetary expectations for requests for more than one per each 12-month period.
Personnel Designations §164.530(a) Administration	***Health care providers must designate a Privacy Official to develop and implement HIPAA privacy policies and procedures. A contact person must be appointed to receive complaints and respond to inquiries relating to internal privacy practices.*** **? Have you designated staff to carry out the role requirements of the HIPAA privacy standards ?** Clarification: Health care providers must name a Privacy Official and designate workforce member(s) to oversee the development and implementation of policies and procedures under HIPAA.	☐ **Yes**	☐ **No**	♦ Designate a knowledgeable workforce member as the Privacy Official and authorize an individual to address privacy complaints. Two different individuals or one in the same can assume these roles. **Sample Policy & Procedure** The practice administrator may be given the title/authority of **Privacy Official** with these responsibilities documented in their job description.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Training §164.530(b) Administration	***A health care provider must train members of its workforce on internal PHI policies and document that training has been provided.*** **? Do you facilitate training sessions to educate staff in handling PHI ?** Clarification: Each workforce member must be promptly trained according to the health care provider's timeframe for implementing policies and procedures for handling PHI.	☐ **Yes**	☐ **No**	♦ Conduct PHI training for existing workforce and new employees upon hire. ♦ Ask workforce members to sign verification of training and maintain copies in personnel files. **Sample Policy & Procedure** Train existing workforce members concurrent with the company compliance timeframe and institute a process for acclimating new staff within 30 days of hire. File documentation in employee personnel files.
Safeguards §164.530(c) Administration	***A health care provider must have appropriate administrative, technical, and physical safeguards in place to protect the privacy and security of PHI from any intentional or unintentional use, disclosure, or regulatory violation.*** **? Do your workforce members have a serious awareness of patient confidentiality practices when handling files, telephone calls, faxing, etc. ?** Clarification: A health care provider must configure its staff, workstations, and files in a manner to safeguard the confidentiality of PHI administratively, technically, and physically.	☐ **Yes**	☐ **No**	♦ Make security awareness part of initial employee training. For example: ▶ Administrative security – training staff to exercise discretion when using PHI in conversations. ▶ Technical security - determining staff PHI access levels through the use of passwords and/or log-on codes. ▶ Physical security – installing locks on unsecured cabinets containing PHI, or housing PHI files in a locked room. **Sample Policy & Procedure** The **Privacy Official** is responsible for ensuring ongoing **PHI** safeguards.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Complaints to the Covered Entity §164.530(d) Administration	***A health care provider must provide a means for individuals to make complaints and/or provide feedback on its compliance of the privacy requirements.*** **? Does your office have a course of action for patient complaints ?** Clarification: A health care provider must document all complaints received by individuals on the handling of their PHI and track disposition.	☐ **Yes**	☐ **No**	♦ Outline steps for filing complaints in the ***Notice of Privacy Practices*** and provide this information to individuals during registration. ♦ Provide individuals with the name of the staff person designated to receive and document PHI-related complaints. **Sample Policy & Procedure** The receptionist/scheduler is responsible for addressing patient complaints. The practice administrator addresses all unresolved complaints. Identify contacts in the **Notice of Privacy Practices.**
Sanctions §164.530 (e) Administration	***A health care provider must affect appropriate sanctions on employees who fail to comply with internal privacy policies or the overall privacy requirements.*** **? Do you have a personnel policy to handle a breach in patient confidentiality ?** Clarification: Employee penalties pertaining to breach in patient confidentiality would not be applicable to disclosures by whistle blowers, workforce members who are victims of crime, or in vindictive circumstances.	☐ **Yes**	☐ **No**	♦ Devote a section of the employee manual to address your organization's policy for dealing with privacy infractions and routinely communicate accountability to workforce members. **Sample Policy & Procedure** Minor **PHI** infractions are handled as a verbal warning and viewed as an opportunity to educate. Gross infractions result in employee termination.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Refraining from Intimidating or Retaliatory Acts §164.530(g) Administration	***A health care provider may not intimidate, threaten, coerce, discriminate, or retaliate against any individual under its care.*** **? Have you prepared your workforce to interact with individuals who choose to exercise their rights under the privacy regulations ?** Clarification: A health care provider must remain neutral towards individuals who choose to exercise their rights under the privacy regulations, including filing a complaint, testifying, assisting, or participating in an investigation, compliance review, or hearing. Individuals have no obligation to participate in any act or practice made unlawful by the regulation, provided the individual has a good faith belief that the health care provider opposed the unlawful act, and that the opposition is reasonable and does not violate disclosure of PHI.	☐ **Yes**	☐ **No**	♦ Offer training programs that clarify the philosophy of management in compliance with the privacy regulations. ♦ Insightfully train workforce members on existing policies in order to avoid indifference when providing patient care. ♦ Immediately report potential situations of non-compliance to the Privacy Official. **Sample Policy & Procedure – Small Provider:** Offer employee training on how to objectively interact with patients who choose to exercise their privacy rights under HIPAA.
Waiver of Rights §164.530(h) Administration	***A health care provider may not condition treatment, payment, enrollment in a health plan, or eligibility for benefits by pressing an individual to waive their right to file a DHHS complaint.*** **? Does your office convey objective behavior and beliefs in regards to HIPAA requirements when interacting with patients ?** Clarification: A health care provider must inform individuals of their right to receive ethical health care in the midst of filing a complaint.	☐ **Yes**	☐ **No**	♦ Include language in the ***Notice of Privacy Practices*** that patients will not be asked to waive their rights to file a complaint with the Department of Health & Human Services as a condition of treatment. ♦ Provide contact information for the Office of Civil Rights in the ***Notice of Privacy Practices.*** ((866)–OCR-PRIV) or (866)627-7748) **Sample Policy & Procedure** Execute the **HIPAA requirements** in a manner that allows individuals to voice their opinion.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Policies and Procedures §164.530(i)(1) Administration	***A health care provider must comply with the elements of the privacy regulations through a development and implementation process.*** **? Have you appointed a workforce member to develop policies and procedures in order to comply with the requirements of HIPAA's privacy standards ?** <u>Clarification:</u> Health care providers are encouraged to proportion policies and procedures according to its size and relevant to its operations using PHI.	☐ **Yes**	☐ **No**	♦ Privacy policies and procedures should be developed in a manner that takes into account the *size* of a health care provider's office and the *types* of PHI use and disclosure. **<u>Sample Policy & Procedure</u>** The practice administrator must conservatively develop and update **PHI** policies and procedures according to the size of the practice.
Changes to Policies or Procedures §164.530(i)(2) Administration	***A health care provider must amend its policies, including the Notice of Privacy Practices, to accommodate changes occurring in HIPAA law.*** **? Have you designated a Privacy Official to maintain and update policies and procedures that carry out the requirements of the HIPAA privacy standards ?** <u>Clarification:</u> A health care provider must implement or change its existing policies and procedures to comply with the HIPAA privacy regulations and any modifications occurring in the law.	☐ **Yes**	☐ **No**	♦ The Privacy Official is responsible to monitor changes in the law, update relevant policies, workforce training documents, and the communication of new information to workforce members. **<u>Sample Policy & Procedure – Small Provider:</u>** The practice administrator is responsible for revising policies and procedures to reflect changes in the **HIPAA** requirements. The **Notice of Privacy Practices** *<u>must</u>* be kept current with existing office protocol.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Changes to Privacy Practices Stated in the Notice of Privacy Practices §164.530(i)(4) Administration	***Unless the right to change a privacy practice has been addressed in the Notice of Privacy Practices, an organization is restricted to handling PHI under the originally described terms.*** **? Are you familiar with what must be done to make changes to your Notice of Privacy Practices ?** Clarification: A health care provider may change policy or procedure that does not materially affect the content of the Notice of Privacy Practices at any time. Substantive changes must be documented and implemented with a new effective date and updates communicated to individuals.	☐ **Yes**	☐ **No**	♦ Include language in the ***Notice of Privacy Practices*** to reserve the right to make changes in the notice. ♦ Describe in detail how substantial changes will be implemented and communicated to patients. **Sample Policy & Procedure** The practice administrator is responsible for validating contents in the **Notice of Privacy Practice**, including an effective date.
Documentation §164.530(j) Administration	***A health care provider must maintain its policies and procedures in written or electronic form for six years from the date of creation, or from the date when the policies and procedures became effective, which ever is later.*** **? Have you considered a way to manage policy information so that the last six years can be accessed and pertinent changes can be detected ?** Clarification: All regulatory requirements must be documented and maintained in written or electronic form for six years.	☐ **Yes**	☐ **No**	♦ Organize HIPAA policies in written or electronic form so they are accessible to workforce members. ♦ Index policies so that revisions can be detected to comply with the six year retention rule. ♦ Annually issue copies of policies to workforce members. **Sample Policy & Procedure** The practice administrator is responsible for maintaining current copies of policies and procedures. Revisions must be chronicled in volumes for referencing changes occurring over a six year span.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Retention Period §164.530(j)(2) Administration	***A health care provider must retain documentation required by regulation for six years from the date of its creation or its effective date, whichever is later.*** **?** ***Do you have date sensitive standards for all documentation in written and/or electronic format ?*** Clarification: A health care provider must retain written and electronic documentation for six years.	☐ **Yes**	☐ **No**	♦ Include a purge date on all written and electronic documentation. **Sample Policy & Procedure** **PHI** should be accessible to the practice for a period of six years from its creation or effective date.
Prior Consents and Authorizations §164.532 (a) Administration	***A health care provider is lawfully permitted to continue the use or disclose of PHI on individuals who have authorized permission prior to the regulatory compliance date provided the individual's specified limitations are honored.*** **?** ***Are workforce members aware of how the implementation of HIPAA will affect current office policies ?*** Clarification: Under HIPAA, the following PHI uses and disclosures are permitted without authorization: (1) use for the health care provider's own treatment purposes, payment purposes, and health care operations; (2) disclosure to a health care provider in order for them to receive payment for their services; (3) disclosure to another health care provider for health care operations such as quality assurance, case management, accreditation, certification, or licensing; or (4) disclosure to health care plan for payment purposes.	☐ **Yes**	☐ **No**	♦ Increase workforce awareness and understanding of the necessary changes to current policy in order to meet HIPAA requirements. **Sample Policy & Procedure** **PHI** must comply with HIPAA requirements for authorization to release information.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Compliance Dates for Initial Implementation of the Privacy Standards §164.534 Administration	***Health care providers, clearinghouses, and most health plans must comply with the privacy regulations on or before April 14, 2003.*** **? Are you preparing to meet the compliance deadline ?** Clarification: Small health plans ($5,000,000 or less in revenue) must comply with the regulations as of April 14, 2004.	☐ **Yes**	☐ **No**	♦ Contact business associates to coordinate timely compliance. **Sample Policy & Procedure** The practice administrator is responsible for assuring timely compliance with the **HIPAA** privacy requirements.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
General Rule and Exceptions – State Law §160.203 Administration	***Conflicting state law that provides more protection for the patient preempts HIPAA.*** **? Are you following state laws in instances where state laws are more stringent than HIPAA concerning confidentiality of patient information ?** Clarification: There are four exceptions to this general rule: (1) DHHS Secretary determines that the state law, regulation, or rule is necessary to prevent fraud and abuse related to due payment for health care; (2) to ensure state regulations governing insurance and health plans as authorized by statute; (3) for state reporting on health care delivery or cost; (4) DHHS Secretary can make a determination for purposes of serving public health, safety, or welfare. State law is more stringent when it (1) prohibits or restricts a use or disclosure that the regulation would permit; (2) grants greater rights of access or amendment to an individual's own PHI; (3) allows a greater disclosure of information than the individual requested; (4) requires restrictive consents or authorizations; (5) requires more detailed record keeping; and, (6) provides supplementary privacy protection over the federal standards. With respect to parents and minors, HIPAA yields to state law unless it is silent.	☐ **Yes**	☐ **No**	♦ Research and become familiar with state law on medical records confidentiality. ♦ Hold training sessions to acquaint workforce members with state laws that supersede HIPAA requirements when it provides greater protections to individuals. **Sample Policy & Procedure** Maryland law that is more stringent, (i.e. provides more protection for the individual) than **HIPAA** takes precedence over the federal legislation. In situations where **HIPAA** regulations are more stringent, or state law is unclear, **HIPAA** precedes state law.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Complaints to the Secretary of HHS §160.306 Administration	***Any person who believes that a health care provider is not complying with the requirements of HIPAA may file a complaint with the Secretary of DHHS.*** **? Does your Notice of Privacy Practices explain an individual's right to file a complaint with the Secretary of DHHS ?** Clarification: Complaints to the Secretary of DHHS must be written or in electronic format. Complaints must include the health care provider contact information and the nature of the violation.	☐ **Yes**	☐ **No**	♦ Include a section in the ***Notice of Privacy Practices*** on filing complaints with the DHHS. ♦ Advise patients during the registration process of the right to file a complaint and the appropriate steps. **Sample Policy & Procedure** Include DHHS complaint and contact information in the ***Notice of Privacy Practices***.
Requirements for Filing Complaints §160.306(b) Administration	***An individual must file a complaint within 180 days of knowing or perceived knowing that the act or omission occurred, unless the time limit is waived by the Secretary of DHHS for good cause shown.*** **? Does your Notice of Privacy Practices outline a specific time frame for filing complaints with the Secretary of DHHS ?** Clarification: Individuals seen by a health care provider must be advised on the time frame in which they are permitted to file a complaint with the Secretary of DHHS.	☐ **Yes**	☐ **No**	♦ Include a section in the ***Notice of Privacy Practices*** on filing complaints with the DHHS. ♦ Advise patients during the registration process of the right to file a complaint, appropriate steps, and time frame. **Sample Policy & Procedure** Include the 180-day time frame for filing complaints in the **Notice of Privacy Practices** and inform individuals of their responsibility to file timely.

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Responsibilities of Covered Entities: Provide Records and Compliance Reports §160.310 Administration	***Health care providers are required to keep records of HIPAA compliance and must be prepared to submit compliance reports to the Secretary of DHHS that validate regulatory compliance.*** **? Would your office be able to respond to an unannounced request for information and documentation from the Secretary of DHHS ?** Clarification: In the event of a DHHS audit, a health care provider must be able to provide documentation of its privacy policies, procedures, and records on individuals.	☐ **Yes**	☐ **No**	♦ Outline goals to achieve HIPAA compliance. ♦ Delegate a Privacy Official. **Sample Policy & Procedure** The practice administrator is responsible for accurate record keeping of **HIPAA** compliance.
Responsibilities of Covered Entities: Cooperate with Complaint Investigations and Compliance Reviews §160.310 (b)(c) Administration	***Requires a health care provider to cooperate with the Secretary of DHHS during investigations or compliance reviews of policies, procedures, or practices.*** **? Is your workforce aware that the Secretary of DHHS is permitted access to information and documentation at any time and without notice ?** Clarification: In the event of a DHHS audit, a health care provider must have knowledgeable and informed workforce members to respond to requests for privacy policies, procedures, and records on its handling and maintenance of protected health information on individuals seen.	☐ **Yes**	☐ **No**	♦ Communicate internal and Federal HIPAA compliance standards to all workforce members in the employee manual. **Sample Policy & Procedure** Workforce personnel must fully cooperate with any complaint investigations.

V. ARRA Addendum to HIPAA Privacy Guide

(Effective February 17, 2009)

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Business Associates §164.308 §164.310 §164.312 §164.316 Administration	***Business associates will be subject to HIPAA security provisions and to sanctions for violation of business associate requirements.*** **? Does your Business Associates Agreement include HIPAA security provisions and sanctions for security violations ?** Clarification: Business Associates would become subject to the same requirements as Covered Entities for implementing administrative, physical, and technical safeguards on PHI. In addition, Business Associates would be required to have written policies and procedures covering these requirements. Business Associates would become subject to the same civil and criminal penalties as Covered Entities.	☐ **Yes**	☐ **No**	♦ Prepare a detailed Business Associate Agreement that specifically outlines HIPAA security provisions and sanctions for security violations. ♦ Develop a file with a copy of all Business Associate Agreements and signatures from the vendors acknowledging receipt and understanding of the terms of the agreement. **Sample Policy & Procedure** Business Associate Agreements must include HIPAA security provisions and sanctions, and the signatures from the appropriate representative acknowledging receipt and understanding of these policies.

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Notification in the case of breach Administration	***Federal law now requires consumer notification of data breaches involving "unsecured" PHI. Both Covered Entities and Business Associates must comply.*** **? Does the Covered Entity and Business Associate have policies that notify consumers when a breach of unsecured PHI is discovered and the procedures including timelines when they will notify the consumer and the Secretary of HHS of this breach *?*** Clarification: Notification must be given no later than sixty (60) days of when the breach is "discovered" and a breach is deemed discovered on the first day upon which the breach is known to the entity (including any employee, officer, or other agent, other than the person that committed the breach). The burden of proof of compliance, including compliance with the timeliness of notice, is on the Covered Entity or Business Associate. In addition, notice to the Secretary of HHS is mandatory, and if the breach involves 500 or more individuals, notification must be given immediately. The notification requirements only apply to information that is "unsecured," i.e., that is not secured through the use of a technology or methodology to be specified by the Secretary of HHS within sixty (60) days of the effective date of the law.	☐ **Yes**	☐ **No**	♦ The Covered Entity or Business Associate shall provide written policies that give details on the procedures for notifying a consumer when a breach involving "unsecured" PHI or information not secured through the use of technology is involved. ♦ The policies should include the timeline for notification after a breach is "discovered," and the manner in which the Covered Entity and Business Associate will notify the customer and the Secretary of HHS. ♦ The notification by the Covered Entity or Business Associate shall provide information that complies with the disclosure to the consumer of a breach of their "unsecured" PHI. **Sample Policy & Procedure** The practice administrator should inform the Covered Entity or Business Associate that they have the burden of proof to report known breaches of "unsecured" PHI within the sixty (60) day timeframe.

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Education on Health Information Privacy Administration	***Designation of a regional office privacy advisor in each regional Office of the Department of Health and Human Services by the Secretary and the establishment of education initiative by the Office For Civil Rights within HHS to provide education on health information privacy.*** **? Do you have the name and contact information of your regional office privacy advisor and for the Department of Health and Human Service's Office for Civil Rights to make inquiries related to the privacy rights with using protected health information ?** Clarification: Each regional office of HHS will offer guidance and education to covered entities, business associates, and individuals on their rights and responsibilities related to Federal privacy and security requirements for PHI. The Office for Civil Rights will develop and maintain a multi-faceted national education initiative to enhance public transparency regarding the uses of PHI, including programs to educate individuals about the potential uses of their PHI, the effects of such uses, and the rights of individuals with respect to such uses.	☐ **Yes**	☐ **No**	♦ Retain the name and contact information for the regional office privacy advisor designated by the Secretary of HHS. ♦ Retain the contact information for the Department of Health and Human Services Office of Civil Rights and the office responsible for educating Covered Entities, Business Associates, and individuals on the rights and responsibilities related to Federal privacy and security for protected health information. **Sample Policy & Procedure** Make sure to include the information on the regional office privacy advisor and the HHS Office of Civil Rights in employee handbooks and training manuals.

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Application of privacy provisions and penalties to Business Associates §164.502(e)(2) §164.504(e) Administration	***The Business Associate of a Covered Entity that obtains or creates PHI shall use and disclose this information in compliance with the terms of the signed Business Associate agreement or written arrangement.*** **?** ***Does your Business Associate Agreement include provisions that any wrongful use or disclosure of protected health information is criminal under the Social Security Act.*** **?** Clarification: ARRA clarifies that any Business Associate that violates any provision on the use and disclosure of protected health information is criminal under the relevant provision of the Social Security Act.	☐ **Yes**	☐ **No**	♦ Make sure the Business Associate Agreement includes language that specifically addresses any wrongful use or disclosure of protected health information is criminal under the Social Security Act. ♦ Provide examples on the type of uses or disclosures of protected health information that would be considered criminal under the Social Security Act. **Sample Policy & Procedure** The practice administrator will review the terms of the Business Associate Agreement with respect to the Business Associate's use and disclosure of PHI before signing the written agreement.

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Restrictions on certain disclosures and sales of health information; accounting of certain protected health information disclosures; and access to certain information in electronic format §164.522 §164.502(b)(1) §164.528 §164.508 Administration	***Restrictions on the remuneration for "sale" of Electronic Health Records or Personal Health Information. Covered Entities using electronic health records (EHRs) are required to provide accounting of disclosures of protected health information for treatment, payment, and health care operations. The limited data set becomes a default minimum necessary standard.*** **? Does the Business Associate Agreement document the restrictions on the use of services or health care operations paid out of pocket by the patient? Does the Covered Entity have a procedure in place that provides an accounting on disclosures of PHI for a three year period? Does the Business Associate or Covered Entity use, disclose, or request a default limited data set with respect to protected health information ?** Clarification: Individuals may require Covered Entities not to disclose self payment services or health care operations if the information pertains only to a health care item or service that the individual has paid for out of pocket, unless otherwise required by law. Covered Entities using electronic health records (EHRs) are required to provide accounting of disclosures of protected health information for three (3) years prior to the date on which the accounting is requested. The effective date of this provision is delayed until after January 14, 2014 for Covered Entities that acquired EHRs as of January 1, 2009, or for entities that acquire EHRs after January 1, 2009, the later of January 1, 2011 or the date upon which the entity acquires the EHR. While the Secretary of HHS has 18 months from the signing of the ARRA to develop "guidance" on what constitutes the minimum necessary amount of PHI, a HIPAA Limited Data Set would be the default standard for what complies with the minimum necessary requirement during this interim period. The Limited Data Set is PHI from which all direct patient identifiers have been removed.	☐ **Yes**	☐ **No**	♦ Develop a policy that restricts the disclosure of protected health information that pertains to a health care item or service for which the health care provider involved has been paid out of pocket in full. ♦ The Covered Entity or Business Associate will develop a process that provides an accounting on the disclosure of a consumer's PHI if the Covered Entity or Business Associate uses an electronic health record (EHR). ♦ The Covered Entity or Business Associate will provide the minimum necessary amount to accomplish the intended purpose of use, disclosure, or request for protected health information. ♦ The Covered Entity or Business Associate shall have a policy that prohibits the sale of EHRs or PHI unless one obtains a valid authorization from the individual. **Sample Policy & Procedure** The practice administrator is responsible for determining whether an individual's PHI should: be disclosed for a health care item or service that the consumer paid for out-of-pocket; provide an accounting on the disclosure for a three-year period; include what constitutes a HIPAA Limited Data Set that meets the minimum necessary disclosure requirement of the consumer's PHI.

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Conditions on certain contacts as part of health care operations Subpart E of §164 Administration	***The HIPAA Health Care Operations exception for "marketing" communications is narrowed significantly, if direct or indirect remuneration is received.*** **?** ***Does the Covered Entity or Business Associate have policies and procedures in place that prohibits the receipt either directly or indirectly of remuneration for any PHI of an individual except pursuant to a valid HIPAA authorization ?*** Clarification: The use of PHI for marketing communications are not within the scope of Health Care Operations, i.e., are not permitted without a HIPAA compliant authorization from each individual, unless it is within one of the following three existing exceptions: health related products or services, treatment, or case management or care coordination. This exception is specifically narrowed by a provision that a Covered Entity or a Business Associate is prohibited from receiving direct or indirect payment in exchange for making any of those Health Care Operations marketing communications, except payment to a Business Associate pursuant to a written contract with the Covered Entity or payment disclosed in a HIPAA compliant authorization from the subject individuals. In addition, individuals have the right to opt-out of receipt of a Covered Entity's fund raising communications. Fundraising for the benefit of a Covered Entity is no longer permitted under Health Care Operations.	☐ **Yes**	☐ **No**	♦ Prepare the policies and procedures for marketing communications guidelines that outline the HIPAA standards for allowing the use and disclosure of PHI without authorization. ♦ Provide examples of marketing communications that are allowed and are not allowed. **<u>Sample Policy & Procedure</u>** The practice administrator should approve all requests that involve receipt either directly or indirectly of remuneration for any PHI of an individual unless it is pursuant to a valid HIPAA authorization form.

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Temporary breach notification requirement for vendors Administration	***Vendors of personal health records and their service providers made subject to the same security breach notification requirements as for Business Associates to Covered Entities and for Covered Entities to Individuals.*** **? Do your agreements with vendors of personal health records and with third party providers include consumer notification of data breaches involving "unsecured" PHI ?** Clarification: The ARRA imposes requirements on entities that provide Personal Health Records and to third party providers of services to those entities regarding notification of breaches involving PHI.	☐ **Yes**	☐ **No**	♦ The vendor should provide written policies with details on the procedures for notifying a consumer when a breach involving "unsecured" PHI or information is not secured through the use of technology. ♦ The policies should include the timelines for notification after a breach is "discovered," and the manner in which the vendor will notify the consumer and the Secretary of HHS. ♦ Develop a file with a copy of all Business Associate Agreements and signatures from the vendors acknowledging the policies and procedures on consumer notification of data breaches involving "unsecured" PHI. **Sample Policy & Procedure** The practice administrator should make vendors aware that they are responsible for compliance with consumer notification of data breaches involving "unsecured" PHI.

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Business Associate contracts required for certain entities §164.502(e)(2). §164.308(b) subparts C and E of §164 Administration	***Health Information Exchanges are brought specifically within Business Associate requirements.*** **? Does the Covered Entity or Business Associate have an agreement with a Health Information Exchange or a Regional Health Information Organization ?** Clarification: The ARRA states that an organization that provides data transmission of PHI to a Covered Entity (or its Business Associate) and that requires access to PHI in order to do so (such as a Health Information Exchange, a Regional Health Information Organization, e-prescribing Gateway, or each vendor that contracts with a Covered Entity) to allow that Covered Entity to offer a personal health record to patients, is a Business Associate of the participating Covered Entities.	☐ **Yes**	☐ **No**	♦ Prepare a detailed Business Associate Agreement with information that specifically outlines the HIPAA security provisions and sanctions for security violations. **Sample Policy & Procedure** A signed Business Associate Agreement is required for the release of PHI to the health information exchange or regional health information organization acknowledging the terms of this agreement.

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Clarification of application of wrongful disclosures criminal penalties 42 U.S.C. 1320d-6(a), Social Security Act Administration	***Specifically clarifies that a violation in obtaining or disclosing individually identifiable health information is criminal under the Social Security Act.*** **? Does your Business Associate Agreement include provisions that any wrongful disclosure of individually identifiable health information is criminal under the Social Security Act ?** Clarification: ARRA clarifies that wrongful disclosures of individually identifiable protected health information are criminal, under the relevant provision of the Social Security Act.	☐ **Yes**	☐ **No**	♦ Develop policies and procedures that address the wrongful disclosure of individually identifiable health information. ♦ Provide examples of what is considered wrongful disclosure of individually identifiable health information. **Sample Policy & Procedure** Have employees sign a statement acknowledging that the wrongful disclosure of individually identifiable health information is a criminal offense under the Social Security Act and provide reminders of this policy during employee training sessions.

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Improved enforcement 42 U.S.C. 1320d-5 Social Security Act Administration	***The Act provides for "Improved Enforcement." The Secretary may enforce and impose set penalties for violations of HIPAA due to "willful neglect."*** **? Do you fully comply with HIPAA and have policies in place that will circumvent violations of HIPAA due to "willful neglect" ?** Clarification: Amends the Social Security Act to add a provision requiring the Secretary to formally investigate any complaint of a violation of this part if a preliminary investigation of the facts of the complaint indicates such a possible violation due to willful neglect." Any violation by a Covered Entity (or its Business Associates) is subject to enforcement and set penalties for violation of HIPAA due to "willful neglect."	☐ **Yes**	☐ **No**	♦ Carefully review the use and disclosure of PHI practices with employees. ♦ Clearly indicate what practices are considered in compliance and provide examples of "willful neglect" to your employees. **Sample Policy & Procedure** Review the practice's procedures in using and disclosing PHI and in maintaining compliance with HIPAA Privacy Rules.

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Audits Subparts C and E of §164 Administration	***The Secretary shall provide for periodic audits to ensure compliance with HIPAA.*** **? Are you prepared to handle an audit by HHS of your privacy policies and procedures ?** Clarification: Requires the Secretary of Health and Human Services to conduct periodic audits of both Covered Entities and Business Associates to ensure HIPAA compliance.	☐ **Yes**	☐ **No**	♦ Prepare a manual that documents the policies and procedures and the documentation that supports compliance with HPAA Privacy Rules. ♦ Provide copies of the HIPAA Privacy Rules in the employee handbook and reminders in publications or signage. **Sample Policy & Procedure** Provide scheduled training and refresher courses to employees on compliance with HIPAA Privacy Rules.

PRIVACY READINESS SELF ASSESSMENT

Of the 44 questions, I would rank my office to be:

_____ **Mostly compliant** (41-44 "yes" responses)

_____ **Somewhat compliant** (36-40 "yes" responses)

_____ **Not at all compliant** (<36 "yes" responses)

Blank Page

VI. Developing a Business Associate Contract

For example purposes only
(Business Associate Contract)

? Who are "Business Associates?"

Business Associates include people or entities that use or disclose protected health information to perform functions and/or assist health care providers. Business Associates are required to adhere to the same standards as the health care provider in handling protected health information.

? Who is responsible for managing the services performed by "Business Associates?"

Health care providers are expected to make sure that privacy protections are maintained whenever subcontracting services that require sharing protected health information. Health care providers are required to investigate complaints received or other information containing substantial and credible evidence of violations by a business associate. Should a health care provider become aware of a substantial violation, they are further required to take reasonable steps to correct the breach and/or terminate the contract.

? Are there circumstances where treatment information can be shared without a business associate contract?

Yes, a Business Associate Contract is not necessary between practitioners or facilities in the treatment of a patient.

? Is legal counsel required to develop a Business Associate Contract?

No, a Business Associate Contract can be independently drafted and implemented. A thorough review of the language is recommended prior to executing and you may choose to solicit legal counsel to perform this task.

? What are the main elements in developing a Business Associate Contract?

- Plainly state the nature of the agreement. Stress the Business Associate's responsibility not to use or disclose the information provided or made available by the health care provider for any purpose other than that expressly permitted under the contract. Clarify that the rights of the information are and remain the property of the health care provider.
- Detail situations within the scope of the provided services where a health care provider or business associate would be permitted to disclose information. Examples of these types of conditions are for claims processing or administration, data analysis, utilization

review, quality assurance, billing, benefit management, practice management, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

- State circumstances where a Business Associate would be permitted to use or disclose information in order to perform their function, such as for management and administration or legal services. Include language stipulating the Business Associate's responsibility for assuring that the third party to whom the information is disclosed exercises full confidentiality and consents to no further disclosure other than stated in the contract, or as required by law. Note: Business Associates are permitted to provide data aggregation services relating to the health care operations of the health care provider.
- Clearly state expectations for safeguarding the use and/or disclosure of the shared information. Some examples:
  - *Administrative Safeguards* – using consistent confidentiality practices when handling patient files and using discretion when transmitting patient information by phone or fax.
  - *Physical Safeguards* – adding manual locks to unsecured cabinets that house protected health information or storing medical files in a locked room.
  - *Technical Safeguards* – instituting password protection of computers in order to access electronic files containing protected health information.
- State the Business Associate's responsibility to grant an individual access to his/her protected health and specify the individual's right to amend their information according to regulations. Require that a log be kept in the individual's medical file of any and all amendments and/or disclosures of protected health information.
- Incorporate language to outline the termination of the contract. Specify expectations for returning or destroying the shared information and your right to immediately terminate the contract if a violation of the privacy regulations is discovered.
- Stress the dual application of the regulations to third party vendors. Clearly state that the terms of the contract apply to all parties, including subcontractors of Business Associates. Require that the Business Associate report known *unauthorized* uses or disclosures of the shared information is under contract. Outline measures that will be taken if employees, subcontractors or agents of the Business Associate are found to be in violation.
- Include language to address a Business Associate's responsibility in the event of a Federal audit by the Secretary of DHHS. The DHHS audits would likely consist of the use and disclosure of personal health information received from or created by the Business Associate on behalf of health care provider.

Business Associate Contract
MODEL FORM

For example purposes only
(Business Associate Contract)

THIS CONTRACT

Entered into on this _____ day of _____, 20___, between

_____ and
(Health Care Provider)

_____.
(Business Associate)

WITNESSETH

WHEREAS, HEALTH CARE PROVIDER will make available and/or transfer to BUSINESS ASSOCIATE certain information, in conjunction with goods or services that are confidential and must be afforded special treatment and protection. WHEREAS, BUSINESS ASSOCIATE will have access to and/or receive from HEALTH CARE PROVIDER certain information that can be used or disclosed only in accordance with this Contract and the Department of Health and Human Services privacy regulations.

HEALTH CARE PROVIDER and BUSINESS ASSOCIATE AGREE AS FOLLOWS:

1. To the limitations on use and disclosure as established under the terms of this contract.
2. BUSINESS ASSOCIATE hereby agrees to refrain from the use or disclosure of the information provided or made available other than as expressly permitted or required under this contract.

The term of this **Contract** shall commence as of _____and shall expire when all
(Effective Date)
information provided by the HEALTH CARE PROVIDER to BUSINESS ASSOCIATE is destroyed or returned to the health care provider.

THE PARTIES HEREBY AGREE that BUSINESS ASSOCIATE shall be permitted to use and/or disclose information provided or made available from the health care provider for the following stated purposes:

_____
_____
_____

Please note: The above-listed uses and disclosures must be within the scope of BUSINESS ASSOCIATE'S representation of HEALTH CARE PROVIDER.

Additional purposes for which BUSINESS ASSOCIATE may use or disclose information:

1. BUSINESS ASSOCIATE is permitted to use information if necessary to properly manage and/or administer its commerce, or if required to carry out legal responsibilities of BUSINESS ASSOCIATE provided the disclosure is required by law.

2. BUSINESS ASSOCIATE is permitted to use or disclose information to provide data aggregation services relating to the health care operations of the health care provider (defined by 45 C.R.R.164.501).

3. BUSINESS ASSOCIATE will establish and maintain appropriate safeguards to prevent the use or disclosure of information.

REPORTS OF IMPROPER USE OR DISCLOSURE

BUSINESS ASSOCIATE hereby agrees to immediately report to HEALTH CARE PROVIDER any and all discovery, use, or disclosure of information not specified in this contract.

SUBCONTRACTORS AND AGENTS EMPLOYED BY BUSINESS ASSOCIATE

BUSINESS ASSOCIATE hereby agrees that any and all information provided or made available to its subcontractors or agents is subject to approval of HEALTH CARE PROVIDER and that any third party agreement shall be executed under same terms, conditions, and restrictions on use and disclosure of information as agreed upon in this contract between HEALTH CARE PROVIDER and BUSINES PROVIDER.

RIGHTS OF INDIVIDUALS TO ACCESS INFORMATION

BUSINESS ASSOCIATE hereby agrees to make available and provide individuals the right to access protected health information in accordance with 45 F.R.R. 164.524. An agreement to release information is subject to the terms of this contract, and BUSINESS ASSOCIATE may use the same contract language substituting its name in place of "HEALTH CARE PROVIDER," where appropriate.

BUSINESS ASSOCIATE agrees to cooperate in making protected health information available to individuals for amendment and agrees to document explicit modifications by the individual in accordance with 45 C.F.R. 164.526.

BUSINESS ASSOCIATE agrees to provide an account of protected health information disclosures to an individual in accordance with 45 C.F.R. 164.528.

RIGHT TO ACCESS BY THE FEDERAL GOVERNMENT'S DEPARTMENT OF HEALTH AND HUMAN SERVICES:
BUSINESS ASSOCIATE hereby agrees to make its internal practices, books, and records relating to use or disclosure of information gained or received under terms of this contract available to the Secretary or the Secretary's designee for purpose of determining compliance with privacy regulations under the Health Insurance Portability and Accountability Act.

MITIGATION PROCEDURES: BUSINESS ASSOCIATE agrees to have procedures in place to alleviate, to maximum extent practicable, any deleterious effects from use or disclosure of protected health information in a manner

contrary to terms of this contract or according to privacy regulations under the Health Insurance Portability and Accountability Act.

SANCTION PROCEDURES: BUSINESS ASSOCIATE agrees to develop/implement a punitive course of action for its employees, subcontractors, or agents who violate terms of this contract or privacy regulations under the Health Insurance Portability and Accountability Act.

PROPERTY RIGHTS: Shared information, including de-identified protected health information, shall be and remains property of HEALTH CARE PROVIDER. BUSINESS ASSOCIATE agrees that it acquires no title or rights to an individual's protected health information as a result of this contract.

CONTRACT TERMINATION: BUSINESS ASSOCIATE agrees that the HEALTH CARE PROVIDER has right to immediately terminate contract and seek relief under Disputes Article if the HEALTH CARE PROVIDER determines that BUSINESS ASSOCIATE has violated a material term of this contract.

RETURN OR DESTRUCTION OF INFORMATION: Upon contract termination, BUSINESS ASSOCIATE hereby agrees to return or destroy all information received or created on behalf of HEALTH CARE PROVIDER. BUSINESS ASSOCIATE agrees not to retain any copies of information after termination of contract. If return or destruction of the information is not feasible, BUSINESS ASSOCIATE agrees to extend protections outlined in this contract and agrees to limit all further use or disclosure. BUSINESS ASSOCIATE agrees to provide HEALTH CARE PROVIDER with written authorization for destroyed information.

GROUNDS FOR BREACH: Non-compliance by BUSINESS ASSOCIATE with any terms of this contract or privacy regulations under the Health Insurance Portability and Accountability Act will automatically be considered grounds for breach.

DISPUTES: Any controversy or claim arising from or relating to the terms defined under this contract are subject to settlement by compulsory arbitration in accordance with the Commercial Arbitration Rules of the American Arbitration Association, except for injunctive relief.

INJUNCTIVE RELIEF: Notwithstanding any rights or remedies provided for in this contract, HEALTH CARE PROVIDER retains all rights to seek injunctive relief to prevent or stop unauthorized use or disclosure of information by BUSINESS ASSOCIATE or any agent, contractor, or third party that received information from BUSINESS ASSOCIATE.

NOTICES: Under the terms of this contract, either party shall be deemed as being given notice if mailed first class United States mail, postage prepaid:

Company Name: _____

Address: _____

Contact Person: _____

Title: _____

NOTIFICATION OF CHANGE OF ADDRESS: HEALTH CARE PROVIDER or BUSINESS ASSOCIATE may at any time change its address for notification purposes by mailing a notice stating change and setting forth the new address.

GOOD FAITH: Parties agree to exercise good faith in performance of this contract.

ATTORNEY FEES: Each party agrees to bear its own legal expenses and any other cost incurred for actions or proceedings brought about by enforcement of this contract, or from an alleged dispute, breach, default, misrepresentation, or injunctive action associated with the provisions of this contract.

ENTIRE AGREEMENT:

- **The terms of this contract consist of this document and constitute the entire agreement between the stated parties.**

- **The terms of this contract shall be binding on the parties. Neither party has the authority to reassign this agreement without the other's written consent.**

IN WITNESS WHEREOF:

BUSINESS ASSOCIATE and ***HEALTH CARE PROVIDER*** have caused this contract to be signed and delivered by their duly authorized representatives, as of _____.
(Date)

BUSINESS ASSOCIATE

Signature _____

Print Name _____

Title _____

HEALTH CARE PROVIDER

Signature _____

Print Name _____

Title _____

VII. Developing a Notice of Privacy Practices

For example purposes only
(Notice of Privacy Practices)

? What is a "Notice of Privacy Practices?"

A "Notice of Privacy Practices" defines how a practitioner office or medical facility administers patient medical information. This document provides the distinctive opportunity to outline office policy in handling patient information and to explain one's rights to access, use, and disclosure of one's personal medical information.

? How often can I modify my "Notice of Privacy Practices?"

The Notice of Privacy Practices can be modified at any time. However, the practice is required to notify all patients seen in the office of updates.

? How can I communicate the "Notice of Privacy Practices" to my patients?

The Notice of Privacy Practices should be part of the registration process for new patients and given to existing patients upon their next visit. Although costly, it can also be mailed to all individuals seen in the office. The Notice of Privacy Practices should be displayed prominently in the waiting area of the office. It can be posted on the wall, placed on tables, or exhibited to the practices' preference.

Best Practices - Development Guidelines:

- Begin the Notice of Privacy Practices with the statement, "This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully."
- Include a description, with at least one example of each, to explain how a health care provider may use or disclose protected health information for treatment, payment, and health care operations.
- Describe the uses and disclosures for which consent, authorization, or the opportunity to agree or object is not required for the release of protected health information. These include standard uses and disclosures that are:

- (1) required by law; (2) for public health activities; (3) for individuals exposed to or at risk of contacting or spreading communicable disease; (4) for the employer's specific purposes (i.e. work-related illness/injury).
- Indicate the manner that an individual may be contacted with appointment reminders, information about treatment and/or treatment alternatives, or other health-related benefits and services.
- State the manner that an individual may be contacted by the office for the purpose of fund raising events.
- Describe an individual's rights in the handling of their protected health information and explain how they can exercise those rights, for example:
  - ♦ To request restrictions on certain uses and disclosures of protected health information. Clearly state that the practice is not required to agree to the requested restriction(s).
  - ♦ To receive confidential communication of protected health information by alternative means or at alternative locations.
  - ♦ To inspect and copy their health information.
  - ♦ To an accounting of disclosures of their health information.
  - ♦ To request a paper copy of a notice originally sent or received electronically.
- **Outline the duties of the office and include:**
  - ⇒ A statement describing the lawful obligation to maintain the privacy of protected health information.
  - ⇒ A statement that the practice is bound by the terms of the notice currently in effect.
  - ⇒ A statement that outlines how future changes to the Notice of Privacy Practices will be affected and how an individual shall be notified of the revisions.
  - ⇒ A statement that other uses and disclosures shall be made only with the individual's written authorization and that the individual may revoke such authorization as provided by C.F.R. 164.508(b)(5).

Notice of Privacy Practices
MODEL FORM

For example purposes only
(Notice of Privcy Practices)

Effective Date: _____

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT AN INDIVIDUAL MAY BE USED AND DISCLOSED AND HOW ONE CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Understanding your health record

A record is made each time an individual visits a hospital, physician, or other health care provider. Symptoms, examination and test results, diagnoses, treatment, and a plan for future care are recorded. This information is most often referred to as the "health or medical record," and serves as a basis for planning an individual's care and treatment. It also serves as a means of communication among any and all other health professional who may contribute to the individual's care. Understanding what information is retained in a person's record and how that information may be used will help you to ensure its accuracy, and enable one to relate to who, what, when, where, and why others may be allowed access to their health information. This effort is being made to assist an individual in making informed decisions before authorizing disclosure of medical information to others. Use or disclosure of a person's health information will follow more stringent State or Federal laws.

Understanding your health information rights

A health record is the physical property of the health care practitioner or facility that compiled it but the content is about an individual and therefore belongs to that individual. One has the right to request restrictions on certain uses and disclosures of information, and to request that amendments be made to their health record. An individual's rights include being able to review or obtain a paper copy of their health information, and to be given an account of all disclosures. One may also request that communications of their health information be made by alternative means or to alternative locations. Other than activity that has already occurred, an

individual may revoke any further authorizations to use or disclosure of their health information.

Our responsibilities

The practice is required to maintain the privacy of an individual's health information and to provide them with notice of the legal commitment and privacy practices with respect to the information collected and maintained about the individual. The office is required to abide by the terms of the notice and to inform the individual if they are unable to grant requested restrictions or reasonable desires of communicating health information by alternative means or to alternative locations.

The office reserves the right to change its practices and effect new provisions that enhance the privacy standards of all patient medical information. In the event that changes are made, the office will notify the individual at the current address provided in their medical file. If applicable, the office will post changes on its web site that provides information about customer service and/or benefits.

Other than for reasons described in this notice, the practice agrees not to use or disclose any health information without the individual's authorization.

To receive additional information or report a problem

For further explanation of this notice you may contact _____ at _____. ⇦ *(Fill in blanks with Privacy Official's Name & Telephone Number).*

If an individual believes their privacy rights have been violated, they have the right to file a complaint with the practice by contacting the individual above, or by contacting the Secretary of Health and Human Services, with no fear of retaliation by the practice.

Your health information will be used for treatment, payment, and health care operations.

Treatment – Information obtained by the health practitioner in the office will be recorded in an individual's medical record and used to determine the best course of treatment consisting of the physician's recorded expectations and those of others involved in providing the individual's care. Sharing of health information may progress to others involved in that individual's care, such as specialty physicians or lab technicians.

Payment – The individual's health care information shall be provided for receiving payment for services rendered by the practice. A bill may be sent to the individual or a third-party payer with accompanying documentation that identifies that individual and their diagnosis, procedures performed and supplies used.

Health Care Operations – The medical staff in the office shall use the individual's health information to assess care received and outcome of the case compared to others like it. Information may be reviewed for risk management or quality improvement purposes in the efforts to continually improve the quality and effectiveness of the care and services provided by the practice.

Understanding our office policy for specific disclosures

- ***Business Associates –*** Some or all of an individual's health information may be subject to disclosure through contracts for services to assist the practice in providing health care. For example, it may be necessary to obtain specialized assistance to process certain laboratory tests or radiology images. To protect the individual's health information, Business Associates are required to follow the same standards held by the office through terms detailed in a written agreement.
- ***Notification –*** A health record may be used to notify or assist family members, personal representatives, or other persons responsible for the individual's care to enhance their well being or whereabouts.
- ***Communications with Family –*** Using best judgment, a family member, or close personal friend, identified by a person, may be given information relevant to their care and/or recovery.
- ***Funeral Directors –*** Health information may be disclosed consistent with laws governing mortician services.
- ***Organ Procurement Organizations –*** Health information may be disclosed consistent with laws governing entities engaged in the procurement, banking, or transplantation of organs for the purpose of tissue donation or transplant.
- ***Marketing –*** The health care provider reserves the right to contact the individual with appointment reminders or information about treatment alternatives and other health-related benefits that they believe is appropriate to the individual.
- ***Fund Raising –*** The health care provider reserves the right to contact the individual as part of fund-raising efforts.

  Patient Directory (typically applicable only to inpatient settings) – Unless the individual objects, the health care provider may use that person's name, room number, general condition, and religious affiliation for directory purposes. This information shall be made available to the clergy and others who ask for the individual by name.
- ***Research (typically applicable only to inpatient settings) –*** Information shall be disclosed to researchers upon the Institution's Review Board approval, and upon the assurance that established protocol to ensure the privacy of the individual's health information has been obtained.

- ***Food and Drug Administration (FDA) –*** The practice is required by law to disclose health information to the FDA related to any adverse effects of food, supplements, products, and product defects for surveillance to enable product recalls, repairs, or replacements.
- ***Worker's Compensation –*** The practice will release information to the extent authorized by the law in matters of worker's compensation.
- ***Public Health –*** The practice is required by law to disclose health information to public health and/or legal authorities charged with tracking reports of birth and morbidity. The office is further required by law to report communicable disease, injury, or disability.
- ***Correctional Facilities –*** The practice shall release medical information on incarcerated individuals to correctional agents or institutions for the necessary welfare of the individual or for the health and safety of other individuals. The rights outlined in this Notice of Privacy Practices will not be extended to incarcerated individuals.
- ***Law Enforcement –*** (1) Health information shall be disclosed for law enforcement purposes as required under state law or in response to a valid subpoena. (2) Provisions of Federal law permit the disclosure of an individual's health information to appropriate health oversight agencies, public health authorities, or attorneys in the event that a staff member or Business Associate of the office in good faith believes that there has been unlawful conduct or violations of professional or clinical standards that may endanger one or more patients, workers, or the general public.

NOTICE OF PRIVACY PRACTICES AVAILABILITY: The terms described in this notice will be posted where registration occurs. All individuals receiving care will be given a hard copy.
Please note: If applicable to your practice you may include…"*This notice will be maintained and available for downloading at the following web site address: _____.*"

Patient Comments:

_____
_____
_____
_____
_____
_____

_____ _____
Patient Signature **Date**

VIII. Developing a Computer and Information Usage Agreement

For example purposes only
(Computer and Information Usage Agreement)

? *What is a "Computer and Information Usage Agreement?"*

A Computer and Information Usage Agreement is a contract between a health care provider and its workforce members that outlines expectations in the use of protected health information (PHI) while performing job functions.

? *Is a "Computer and Information Usage Agreement" necessary?*

Yes, having workforce members acknowledge your expectations protects and assures that PHI is handled responsibly within the organization

DEVELOPMENT TIP:

Plainly state expectations of employees having access to PHI in the performance of duties and include information relating to liabilities in handling or removing PHI from the premises, sharing or falsifying information, operating standards of the organization, and system limitations.

Computer and Information Usage Agreement
MODEL FORM

For example purposes only
(Computer and Information Usage Agreement)

_____ considers the
(Insert name of Health Care Provider)
security and confidentiality of protected health information (PHI) a matter of high priority. Any and all members of this organization having access to patient medical files and information will be held solely responsible for safeguarding and maintaining strict confidentiality. In order to be granted access to PHI, you must agree unconditionally to the following standards:

1. To respect the privacy and rules governing the use of accessible information though the computer system and/or network and to only utilize that information necessary in the performance of duties.

2. To respect the ownership of proprietary software by not making unauthorized copies for personal use.

3. To respect the capability of the computer system and be cognizant of its limitations, including any that may interfere with the activity of other users.

4. To respect the procedures established by this organization to govern system use.

5. To advocate security measures in preventing the unauthorized use of information stored physically or electronically by this organization.

6. To not seek personal benefit or permit others to personally benefit from work-related access of confidential information or the use of equipment available in the performance of duties.

7. To resist operating unlicensed software.

8. To maintain the integrity of the information provided by this organization for the fulfillment of duties and to only disclose that which is necessary to complete an assignment or according to organization policy.

9. To protect record content and not include, or cause to be included false, inaccurate, or misleading information.

10. To not remove PHI from where it is housed except in the performance of duties.

11. To not release personally assigned authentication codes or devices toanyone, or allow another access to this information under false pretenses.

12. To not utilize the personal authentication codes or devices of others employed by this organization.

13. To report any violation of this agreement.

14. To handle, maintain, and dispose of patient/member PHI according to the policies established by this organization.

15. To not divulge information that identifies PHI.

I fully understand that the information I may have access to in the performance of my duties contains sensitive and confidential patient-specific details of treatment, payment and the health care operations of this health care provider. In signing this agreement, I acknowledge the responsibility placed on me as an employee of this organization and understand that my access to tangible and automated PHI is subject to the scrutiny of this organization.

_____ _____
(Employee Signature) (Date)

_____ _____
(Witness) (Date)

EMPLOYEE-SPECIFIC COMPUTER
IDENTIFICATION INFORMATION

SERIAL NUMBER _____

MODEL NUMBER _____

LEVEL OF ROLE-BASED ACCESS:

▬Total LAN access

▬Limited LAN access _____
(specify network limitations)

IX. Developing a Patient Acknowledgement Form OPTIONAL

For example purposes only
(Patient Acknowledgement Form)

? *What is a "Patient Acknowledgement Form"?*

A patient acknowledgement form can be used to <u>pointedly</u> ask an individual for their dated signature prior to your office using or disclosing their protected health information to carry out treatment, payment, or health care operations. It is simply an acknowledgement that the Notice of Privacy Practices has been reviewed with the individual and that they are fully aware of policy and procedures practiced by the office covering protected health information received or created that identifies or may identify that individual and pertains to their physical or mental health, the health care provided and/or payment for services.

? *Can I use an existing form and just add the acknowledgement of the Notice of Privacy Practices?*

YES. Like many health care providers, the practice may routinely ask for a patient's consent upon admission to assure their understanding of information disclosures to insurance companies (or other entities) for payment purposes. The privacy rule builds on this practice by establishing a customary routine of obtaining patient consent for uses and disclosure of protected health information about the patient in order to carry out treatment, payment, or health care operations. EXISTING DOCUMENTS MAY BE UPDATED BY INCORPORATING THE HIPAA LANGUAGE.

? *What are the recommended elements for this document to be valid?*

1. MAKE IT BRIEF! The purpose of this document is to make sure the patient understands how the office may use and/or disclose their protected health information to carry out treatment, payment, or health care operations. The specifics of the office procedures must already be defined in the ***NOTICE OF PRIVACY PRACTICES*** and only need to have a patient's acknowledgement that they have received the Notice of Privacy Practices information.
2. State that this authorization is valid throughout the relationship with the patient and plainly state their choice to overturn the agreement <u>in writing</u> at any time.
3. Make sure the form is signed and dated by the individual.
4. Retain the form in the patient's medical file for a minimum of six (6) years.

PATIENT ACKNOWLEDGEMENT FORM
Use & Disclosure of Protected Health Information
MODEL FORM

For example purposes only
(Patient Acknowledgement Form)

_____ "Notice of Privacy
(Name of Health Care Provider)
Practices" provides information about how we may use and disclose protected health information about you. Please acknowledge receipt of this office's Notice of Privacy Practices by initialing below:

_____
Patient's initials

Our Notice of Privacy Practices states that we reserve the right to change the terms described. Should this happen, you will receive a revised copy by mail *(or explain your discretionary terms)*.

_____
Patient's initials

You have the right to request restrictions on how your protected health information may be used or disclosed for treatment, payment, or health care operations. We are not required to agree to your restrictions, but if we do, we are bound by our agreement with you.

_____
Patient's initials

By signing this form, you consent to our use and disclosure of protected health information about you for treatment, payment, and health care operations. You have the right to revoke this consent, in writing, except where we have already made disclosures in trust on your prior consent.

Signature **Date**

X. Developing an Authorization Form

For example purposes only
(Patient Acknowledgement Form)

? What is an "Authorization Form?"

An authorization form is more specific than a consent form and gives permission to use particular protected health information for specified purposes other than for treatment, payment, or health care operations.

? What about the release of mental health records or psychotherapy notes?

The Privacy Rule requires health care providers to obtain authorization to disclose protected health information maintained in psychotherapy notes. The exceptions to this rule (§164.508(a)(2) are:

- Use by the originator of the psychotherapy notes for treatment;
- Use or disclosure by the health care provider in training programs in which students, trainees, or practitioners in mental health learn to practice or improve their skills in group, joint, family, or individual counseling;
- Use or disclosure by a health care provider to defend a legal action or other proceeding brought by an individual.

? What elements must be included in an "Authorization Form?"

1. Specific information being used or disclosed and its purpose
2. Person authorized to disclose information and recipient of information
3. Expiration date or event
4. Statement of the patient's right to revoke
5. Date
6. Signature (and authority of individual if other than patient)
7. Statement of potential for redisclosure

Examples of Situations	Consent? or Authorization?
Supports all uses and disclosures for treatment, payment, and health care operations by a health care provider for an indefinite period of time.	**Consent** – because this information must be addressed in the Notice of Privacy Practices.
Allows health care provider to sell patient mailing list.	**Authorization** – because this release would be for marketing purposes.
Allows health care provider to send an appointment reminder to a patient.	**Consent** – because this office practice must be addressed in the Notice of Privacy Practices.
Allows health care provider to release information to an employer for employment decisions.	**Authorization** – because this is a specific release beyond treatment, payment, or the health care operations of the health care provider.
Allows health care provider to disclose information for eligibility to purchase life insurance.	**Authorization** – because this is a specific release beyond treatment, payment, or the health care operations of the health care provider.

AUTHORIZATION FORM
Use and Disclosure of Protected Health Information
MODEL FORM

For example purposes only
(Authorization Form)

Patient's Name _____

Medical Record or Social Security # _____

1. Persons or group of persons authorized to **use/disclose** this information

2. Persons or group of persons authorized to **receive** this information

3. Description of the information to be used or disclosed:

4. ***This section <u>must</u> be completed if request for disclosure is made by someone other than the above-named patient:***

Purpose for disclosure of information:

I understand that the person I am authorizing to use/disclose my protected health information may receive compensation for doing so.
_____
Patient Initials

I understand that I may refuse to sign this authorization and that if I do, it will not affect my ability to obtain treatment or payment or eligibility for benefits and that I may inspect or copy any information used or disclosed under this authorization. _____
Patient Initials

5. I understand that if the party receiving this information is not a health care provider or health plan subject to the federal privacy regulations that the information described above may be redisclosed and no longer protected by the privacy regulations. _____
Patient Initials

6. I understand that I may revoke this authorization in writing at any time except to the extent that action on this authorization has not already occurred.

7. This authorization becomes effective _____ and will expire on _____.

_____ _____
Patient (or Representative*) Signature Date

_____ _____
Name of Personal Representative (please print) Relationship to Patient

The Center for Health Information Technology
David Sharp, Ph.D.
Director

Website: www.mhcc.maryland.gov
Tel. (410)764-33460 Fax (410)358-1236